EBOOK

3 Steps to Getting Started With Cyber Risk Quantification

WHY IT'S MORE IMPORTANT THAN EVER TO BE ABLE TO QUANTIFY CYBER RISK

In today's ever-evolving security landscape, cyber risk is constantly increasing — making it critical for you to be able to effectively analyze your organization's security performance over time. In a 2020 survey conducted by Harvard Business Review Analytic Services, 74% of 168 executives named cyber risk as one of the top three risks their company faces today. That puts cyber risk well ahead of the next risk category — risk of business disruption and systems failures — which only 42% cited.

Given this increased focus on cyber risk, it's more important than ever to build a strategic security performance management program in which you take a risk-based, outcome-driven approach to measuring, monitoring, managing, and reporting on your organization's cybersecurity program performance over time. In order to do so, you need a framework to assess your exposure to cyber risk and lead meaningful conversations on its business impact with the board and other stakeholders.

This is where cyber risk quantification can have a huge impact, empowering security leaders to build the necessary business context with data-driven metrics that indicate program performance. By presenting this type of data in context, security leaders can provide the board and other stakeholders with the insights they need to make more informed security investment decisions — helping to bridge the gap between security and the business.

FINANCIAL ORGANIZATIONS AS PRIME TARGETS

According to a Boston Consulting Group (BCG) report, financial services firms are 300 times more likely to be targeted by a cyber attack. And these attacks can be costly. In 2020, the president of the European Central Bank (ECB), Christine Lagarde, went on record to warn that a cyber attack on a major financial institution could trigger a liquidity crisis, referring to a European Systemic Risk Board (ESRB) report that estimates the global cost of cyber attacks to be anything up to US$645 billion.

To make matters more complex, a report by Accenture states that almost eight out of 10 business leaders believe that they are adopting new and emerging technologies faster than they can address related security issues. According to Accenture's analysis, the banking sector risks losing an estimated US$347 billion in value creation opportunities to cyber crime over the next five years.

In light of this heightened threat landscape, finance organizations need to have a process in place to continuously monitor their attack surface — enabling them to discover hidden vulnerabilities in their data centers and systems, assess their current security state, analyze how their security performance ranks against industry peers, and create improvement plans to reduce cyber risk. That's where BitSight for Security Performance Management (SPM) comes in — helping security and risk leaders take a risk-based, outcome-driven approach to assessing and managing the performance of their organization's cybersecurity program over time.

QUANTIFYING CYBER RISK AS A BOARDROOM ISSUE

Since the rise of the COVID-19 pandemic, organizations have been reassessing their project portfolio to ensure they are protecting shareholder capital while remaining relevant and effective. As the risk profile of an organization frequently changes, the ability to make quick, data-driven decisions is more important than ever before.

Mature, strategic security performance management programs benefit the enterprise by quantifying the organization's risk profile in a language that makes sense to the business. Doing so empowers the organization to make informed cybersecurity decisions regarding resource allocation and investments by:

- Prioritizing projects aimed at stabilizing the business or meeting the desired risk threshold
- Revisiting the business cases for ongoing projects to help ensure that they are still relevant and aligned with the latest business strategy
- Identifying workarounds to minimize the disruption caused by deferred or canceled projects
- Continuously monitoring the ripple effects of the pandemic and tailoring IT services and solutions to ensure alignment with business goals

Meanwhile, the boardroom is focusing more and more on cybersecurity, prompting an increased need for cyber risk to be measured and reported in financial terms. Business leaders want to know more about the risks that they face, but traditional red-amber-green heat maps and scorecards don't provide sufficient insight. The board and other stakeholders are focused on running the business, and they want to be able to connect cybersecurity data to real business risk.

Today's CISOs must work within the technical realm and the business realm in order to make decisions that protect business interests and empower them to secure the necessary IT budgets. As such, a leading CISO needs to be able to transform the technical side of cybersecurity and information security into financial language.

To put it bluntly, many stakeholders are asking: "How much do we stand to lose financially if we don't address a particular gap in our security program?" Here, it's critical that CISOs can report to the board and other non-technical stakeholders in a language they understand — aligned with how they look at other types of organizational risk and quantified like other initiatives that receive funding.

THE NEED FOR CYBER RISK QUANTIFICATION

In basic terms, cyber risk quantification involves analyzing and assigning data-driven metrics to previously identified cyber risks in order to make decision-making easier. This process puts the intangible nature of 'risk' into tangible business contexts — helping decision-makers make sense of various risk factors so that they can effectively prioritize their remediation efforts.

Cyber risk quantification can be based on various different KPIs, such as security ratings, or modeling techniques used by cyber insurers to assess potential financial exposure. There are various approaches and frameworks, but the ultimate goal of quantitative risk analysis is to present the risk data in business terms so that organizations can make informed decisions regarding security investments and risk mitigation.

Cyber risk quantification can be based on various different KPIs, such as security ratings, or modeling techniques used by cyber insurers to assess potential financial exposure.

Quantifying cyber risk and the impact of implementing specific controls will help today's leading CISOs provide the necessary business context and guide the board's focus towards outcomes. This brings about a host of benefits:

- The board can gain more insight into cybersecurity matters with data-driven metrics and business context
- The entire team can make faster, more informed investment decisions
- CISOs can demonstrate the ROI of implemented solutions in a language that makes sense to the business

Financial quantification of cyber risk allows risk professionals to understand their organization's potential financial exposure due to a cyber event. Some of the benefits of financial quantification are the following:

- Uncovers various implications (tangible and intangible) from a financial standpoint
- Provides a clearer understanding of an organization's probable cyber exposure and its impact
- Enables informed discussion around accepting, mitigating, or transferring of risk through insurance
- Offers a catalyst to increase cybersecurity awareness beyond IT to the rest of the organization
- Informs educated investments in reducing overall cyber exposure

Overall, this changes how cybersecurity is discussed. Now, your board, non-technical stakeholders, and other risk management leaders can better understand and evaluate cybersecurity programs and cyber risk in financial terms. A greater understanding of cyber risk strengthens your Board of Directors' and organizational leadership's ability to deliver better and more secure business outcomes for your investors, business partners, and customers.

3 STEPS TO GETTING STARTED WITH CYBER RISK QUANTIFICATION

The road to sophisticated cyber risk quantification is paved by establishing certain thresholds, policies, and frameworks — with the ultimate payoff of winning the confidence of the CEO, board, and investors in your ability to manage cyber threats while increasing the return on your cybersecurity investments.

1. Define an Acceptable Risk Threshold

Determining what your organization considers to be an acceptable risk threshold is a critical step to developing an effective cyber risk management program. But it's not a decision for security or IT teams to make alone.

Take the following steps to align with the wider team and ensure you're putting the necessary controls in place:

- **Gain visibility into the risk present across your expanding digital ecosystem:** In order to effectively determine your organization's risk appetite, you need to be able to assess what type of risk your organization is exposed to in the first place. With BitSight Security Ratings data, you can continuously monitor your network for vulnerabilities such as unpatched systems, open access ports, and misconfigured software — empowering you to assess your real-time cyber risk across on-premise, cloud, and remote office environments in an efficient and effective way.
- **Interview various stakeholders:** Connect with teams such as legal, finance, and risk management to understand their unique perspectives on the type of risk your organization should accept, mitigate, and transfer.
- **Define the right risk threshold for your business:** Leverage the insights gained from the steps above to establish your risk threshold and put the necessary compliance policies in place. Here, having a standardized, easily understandable KPI like security ratings can be hugely beneficial as you can align on a specific set of standards.

2. Define a Strategy for Measuring and Quantifying Risk

In order to effectively scale your cybersecurity program, you need to have an efficient process for assessing, monitoring, and remediating risk. With a dynamic metric like BitSight Security Ratings, it's easier than ever to hold your cybersecurity program accountable to a quantitative standard. Instead of being an unknown variable, cyber risk becomes as clear as a credit score.

With security ratings as a foundation, business leaders have the opportunity to improve their resource allocation, optimize their cybersecurity program, and, as a result, effectively manage their overall cyber risk over time.

i) Security Ratings and Risk-based Reporting

With this dynamic insight into the real-time state of cyber risk across your organization, you can evaluate the overall effectiveness of your current program, rank areas of critical or disproportionate risk, and prioritize limited resources to achieve the greatest performance impact.

By diving into specific grades for the individual risk vectors that make up a security rating, a CISO can determine which areas are exposing their organization to the greatest amount of cyber risk. Rather than spend time and money receiving diminishing returns on areas where their performance is rated as good or excellent compared to their peers, security leaders can shift resources to areas with more critical need.

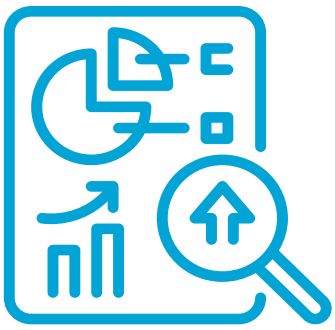
Security ratings can also be used for benchmarking. By comparing your organization's current security rating to past performance, you can accurately gauge whether or not your team's efforts are paying off. This same technique can be used to assess the ROI of expensive cybersecurity technologies or services.

ii) Evaluating Cyber Risk in Financial Terms

Many companies have yet to fully understand what it means to be exposed as a business to cyber risk. They tend to focus on high-impact cyber events such as a malware attack from a technical perspective — and often fail to consider other types of cyber scenarios and the potential business implications.

If you can assess this type of cyber risk from a financial point of view, you can translate the potential cyber risk impact into business terms. This will provide the insight needed to make informed decisions on the type of risk to accept, mitigate, or transfer.

More and more leading CISOs are looking to elevate cyber risk to business risk by quantifying it in financial terms. Here are a few leading frameworks for financial quantification:



Factor Analysis of Information Risk (FAIR)

FAIR provides a model for understanding, analyzing, and quantifying cyber risk and operational risk in financial terms. The FAIR framework is based on the concept that risk is uncertain, and businesses should instead focus on the probability of cybersecurity events. It's an in-depth model that includes their very own risk taxonomy and technical standards. Its probability-based approach can be applied to any type of asset your business works with. The particularity of the FAIR methodology is to transpose each impact to a financial cost (direct, indirect, tangible, and intangible costs).

KOVRR - Cyber Risk Modeling

Kovrr provides leading insurance carriers and reinsurers with an end-to-end cyber risk modelling platform that delivers transparent, real-time, data-driven insights into their cyber risk exposure. The platform is designed to help underwriters, exposure managers, and catastrophe modelers understand, financially quantify, and manage cyber risk by utilizing AI-powered risk models.

Kovrr's technology is based on monitoring global incidents in real time, utilizing the largest and most detailed exposure database in the industry, which contains firmographic and technographic details on millions of businesses worldwide. Kovrr's value lies here: its proprietary databases and modeling techniques. With Kovrr, exposure managers can assess cyber risk exposure across many sources and quantify the potential impact on capital — enabling them to make more strategic decisions.

3. Report on Improvements Over Time to Show ROI

Once you're done with quantifying cyber risk, the next step is to present those metrics to the necessary decision-makers. In the past, a main challenge you may have faced with getting approval for your cybersecurity budgets was likely finding an easy way to show ROI when you're dealing with intangible terms such as low risk or high risk.

Today's CISOs need to do more than try to "sell" their solutions based on probability with no hard numbers. It's more important than ever that they present actionable ROI insights in context. In cyber risk quantification terms, ROI is all about risk mitigation.

ROI

=

HOW MUCH RISK THE SOLUTION IS PROTECTING YOU FROM

VS.

HOW MUCH THE SOLUTION COSTS

In order to demonstrate the impact of your security investments, you need to take a risk-based, outcome-driven approach to security performance management, in which you continuously assess your security posture, visualize areas of disproportionate risk across your ecosystem, and quantify the effectiveness of your security controls. As security ratings are updated on a daily basis, you can use this metric to gain a dynamic view into how your security performance is changing over time. Armed with these insights, you can demonstrate ROI faster and easier than ever before.

MAKING MORE INFORMED, DATA-DRIVEN SECURITY DECISIONS

A key benefit of taking a quantitative approach to cyber risk management is enabling better resource prioritization.

Having quantified data at your fingerprints empowers you to determine which risks to mitigate in order to achieve the greatest security posture impact. This way, you can make more informed cybersecurity decisions regarding resource allocation and investments. Once you have assessed your current security posture and identified the gaps in your security program, you need to prioritize:

- Which gaps would be the most impactful to remediate and would have the best benefit to your security posture?
- How much would the necessary controls cost? Do you have the budget to implement these controls?

A key benefit of taking a quantitative approach to cyber risk management is enabling better resource prioritization: more efficient allocation of people, processes, and budget around the risks that matter most for maximum risk reduction. By putting a price on risk (an organization's potential loss exposure), quantification shows decision makers how alternative tactics compare in the apples-to-apples, financial terms that everyone understands.

Where you see risk as an issue, the decision maker will look at the same risk from the financial perspective and consider the financial viability of your solution. Here, it's all about finding that perfect balance between the costs of running a business and the costs of protecting it.

Major financial services organizations now assess the financial risk that cyber threats pose and put a dollar figure to how much of that risk they are mitigating. By having increased visibility into the likely costs of the cyber risks that potential acquisitions may present, they can now execute their acquisition strategy better and more quickly than ever before.

QUANTIFIED CYBER RISK IS MANAGED CYBER RISK

There's no question about it: cybersecurity is top of mind for the financial services sector. This industry is a high-profile target for cyber threat actors, and cyber risks are a danger to the stability of national and global financial systems.

Through cyber risk quantification, you can bring about an unprecedented awareness and understanding of risk beyond the technology function into the boardroom — where important decisions around risk management and insurance policy are being made. Leveraging a quantification framework empowers you to guide strategic conversations around managing your cyber risk, prioritizing new technology investments, and measuring the ROI of those investments in specific controls or programs.

Of course, in order to make more informed decisions, you need to align as an organization around a standardized KPI through which to assess and discuss your risk exposure in the first place. With BitSight Security Ratings, it's easier than ever to gain real-time insight into your security posture, so you can evaluate the overall effectiveness of your current program, rank areas of critical or disproportionate risk across your digital ecosystem, and prioritize limited resources to achieve the greatest performance impact.

Interested in learning more about how BitSight empowers you to quantify risk and get the most out of your security investments? Go to https://www.bitsight.com/security-performance-management or contact sales@bitsight.com.

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.